Chapitre VIII

Cryptologie

Introduction

Pendant les 2 premières années de la Première Guerre mondiale, le président des Etats-Unis, Woodrow Wilson a refusé avec constance l'envoi de troupes américaines en renfort des Alliés.

Le 17 janvier 1917, les Anglais intercepte un télégramme allemand et parvienne à le déchiffrer.

Ce télégramme annonce l'intention de l'Allemagne de se lancer dans une guerre sous-marine totale et demande une alliance au Mexique.

Introduction

Le 7 mai 1915, un sous-marin allemand (U-Boat) avait torpillé le paquebot *Lusitania*, faisant 1198 victimes civiles, dont 124 américains.

Le président américain avait prévenu son homologue allemand que tout nouvel événement similaire entraînerait l'entrée en guerre des Etats-Unis au côté des alliés.

La guerre totale des sous-marins allemands signifierait certainement des victimes américaines.

Introduction

Dans son télégramme, le ministre allemand Arthur Zimmerman, demandait au Mexique de s'allier à l'Allemagne. De la sorte, les Etats-Unis menacé directement sur leur territoire n'apporteraient pas d'aide aux Alliés en Europe, mais se concentreraient uniquement sur la défense du pays.

Le renseignement et le gouvernement britannique faisait face à un dilemme.

Introduction

D’une part, transmettre l’information au président Wilson entraînerait probablement directement l’entrée en guerre des Etats-Unis ce que les Alliés désiraient. Mais cela informerait aussi l’Allemagne que ses communications secrètes ne l’étaient plus vraiment secrètes et que les Alliés étaient capables de lire tous les messages.

Si les Allemands apprenaient que le code n’est plus protégé, ils le changeraient immédiatement et les Alliés perdraient une source importante d’information.

Introduction

Mais ne pas transmettre l'information aux Etats-Unis, laissait une chance au plan allemand de fonctionner….

De plus, les Britanniques ne pouvaient pas révéler aux Etats-Unis comment ils avaient intercepté le message. Interception via des communications américaines que les britanniques n'étaient pas sensé « écouter ».

Introduction

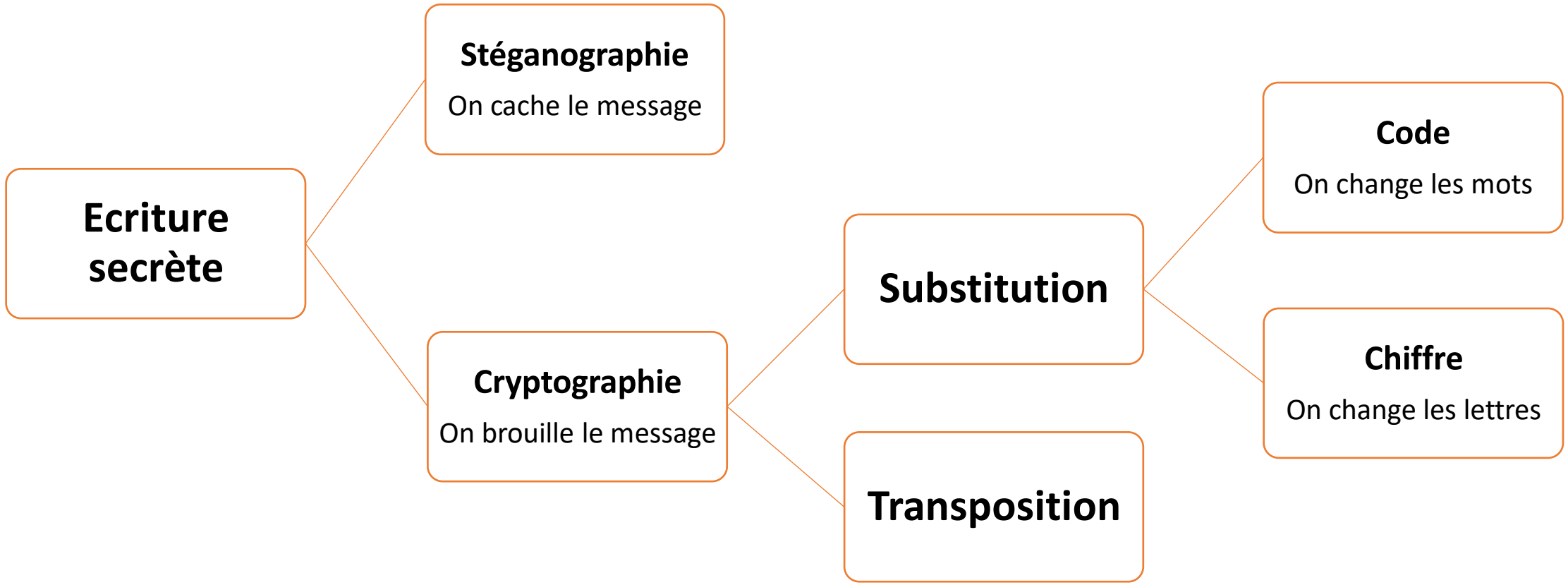
Au final, les Britanniques ont passé l'information aux Etats-Unis mais en prenant soin de faire croire que le message avait été intercepté lors d'une communication entre l'ambassade allemande de Washington et le Mexique.

Cryptologie

La **cryptologie** est la science du « **secret** ».

Elle englobe la **cryptographie** (l'écriture secrète) et la **cryptanalyse** (l'analyse de cette dernière)

Cryptologie



Cryptologie

La **stéganographie** consiste à **dissimuler** le message.

La **cryptographie** consiste à rendre le **message inintelligible**, mais pas de le dissimuler.

Stéganographie

Hérodote rapporte dans ses chroniques des guerres entre les Grecs et les Perses, deux méthodes de stéganographie:

- Histiée, connu comme étant le tyran de la ville de Milet, demanda à un homme de se raser la tête. Il écrivit ensuite le message sur son crâne et attendit que les cheveux repoussent pour l'envoyer comme messager.
- Démarate voulait avertir Sparte du projet d'invasion du roi perse Xerxès. Pour transmettre son message, il gratta la cire d'une tablette et écrivit son message sur le bois de celle-ci. Il recouvrit ensuite la tablette de cire qui permit à son transporteur de se déplacer avec une tablette « vierge »

Stéganographie

Un moyen stéganographique qui a traversé les siècles est celui de l'encre invisible, sous toutes ses formes: jus de citron, sève de plantes ou urine humaine. Ces substances ont une haute teneur naturelle en carbone et ont tendance à noircir lorsqu'elles sont soumises à des températures peu élevées comme la flamme d'une bougie

En Chine ancienne, on écrivait des messages sur de fines bandelettes de soie. La bandelette était ensuite glissée dans une minuscule boule qui était recouverte de cire. Le messager avalait la boule et transportait le message.

Stéganographie

La stéganographie présente un défaut de taille:

Stéganographie

La stéganographie présente un défaut de taille:

Si le message est intercepté, son contenu est transparent

Stéganographie

C’est pourquoi, la stéganographie est utilisée comme complément à la cryptographie, afin de renforcer la sécurité de la transmission.

Application

Comme un arc en ciel, c’est beau,
Orange, vert, rouge, indigo,
Unie, chamarrée, brillante,
La couleur peut être vivante,
Etalée sur la palette,
Unisson des teintes en fête,
Rien n’égale leur harmonie,
Si l’ensemble est bien choisi.

Stéganographie

C’est pourquoi, la stéganographie est utilisée comme complément à la cryptographie, afin de renforcer la sécurité de la transmission.

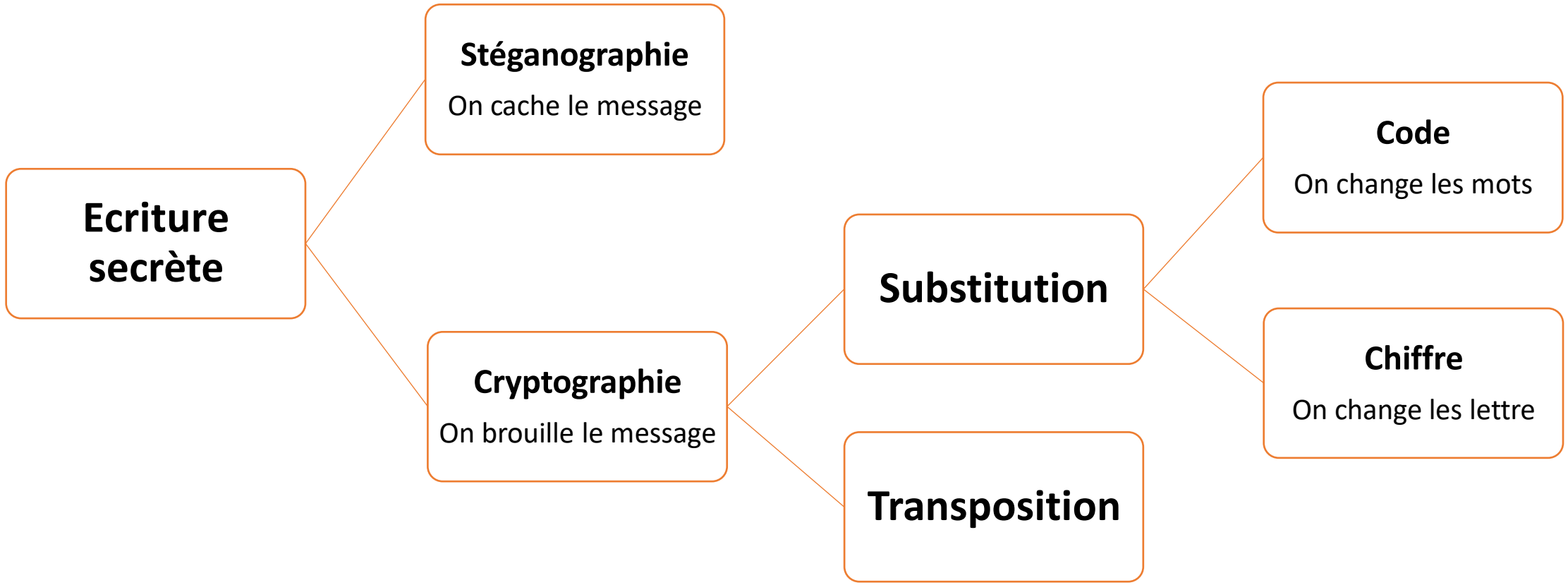
Application

Comme un arc en ciel, c’est beau,
Orange, vert, rouge, indigo,
Unie, chamarrée, brillante,
La couleur peut être vivante,
Etalée sur la palette,
Unisson des teintes en fête,
Rien n’égale leur harmonie,
Si l’ensemble est bien choisi.

Acrostiche

Comme un arc en ciel, c’est beau,
Orange, vert, rouge, indigo,
Unie, chamarrée, brillante,
La couleur peut être vivante,
Etalée sur la palette,
Unisson des teintes en fête,
Rien n’égale leur harmonie,
Si l’ensemble est bien choisi.

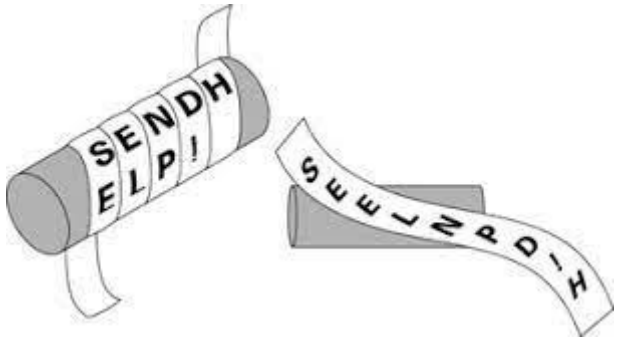
Cryptologie



Transposition

Pendant la guerre qui opposa les Spartiates et les Athéniens, il est devenu habituel d'utiliser de longues bandes de papier sur lesquelles on écrivait le message, une fois ces bandes enroulées sur un bâton: la scytale.

Le chiffrement reposait sur la modification du message original par l'inclusion de symboles inutiles qui disparaissaient lorsque le message était enroulé sur le bâton, de longueur et de grosseur prédéfinies.



Transposition

Même en connaissant la technique utilisée, soit l'algorithme de chiffrement, celui qui interceptait le message avait beaucoup de difficultés à le déchiffrer.

La longueur et la grosseur de la scytale étaient finalement la clé du système.

Transposition

La transposition consiste à mélanger les lettres d'un message pour former des anagrammes:

AHMT

↓

MATH

Pour des petits messages, il est assez facile d'essayer toutes les possibilités pour finalement trouver le message original.

Transposition

Pour des messages plus longs, c’est un peu plus compliqué, mais si on y consacre suffisamment de temps, cela reste assez simple …

TNERTSTNRSNIRIFITDVEDASNRSNIROSCEETOPIONESLUTUEINRSOPIONE

Transposition

Pour des messages plus longs, c'est un peu plus compliqué, mais si on y consacre suffisamment de temps, cela reste assez simple …

TNERTSTNRSNIRIFITDVEDASNRSNIROSCEETOPIONESLUTUEINRSOPIONE

↓

Transposition en dent de scie

T N E R T S T N R S N I R I F I T D V E D A S N R S N I R

O S C E E T O P I O N E S L U T U E I N R S O P I O N E

↓

TON SECRET EST TON PRISONNIER; S'IL FUIT TU DEVIENDRAS SON PRISONNIER

Transposition

Prenons 3 lettres au hasard: A, O et R.

Sans trop d’effort, on voit rapidement qu’il existe plusieurs manières de réorganiser ces trois lettres.

Combien ?

Transposition

Prenons 3 lettres au hasard: A, O et R.

Sans trop d'effort, on voit rapidement qu'il existe plusieurs manières de réorganiser ces trois lettres.

Il existe six manières de réorganiser ces trois lettres: AOR, ARO, OAR, ORA, ROA et RAO.

Une fois choisi un des caractères à la première place sur les trois positions possibles, il nous reste deux caractères qui peuvent être positionnés de deux manières différentes, soit un total de $\mathbf{3 \times 2 = 6\ combinaisons}$.

Transposition

Maintenant, considérons, non plus trois lettres, mais dix lettres. On obtient un nombre de combinaisons

$$10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 10! = 3628800$$

Ainsi pour un message, de taille raisonnable, de 40 caractères, il y a un nombre combinaisons possibles qu'il devient inenvisageable de vérifier une à une.

La transposition est-elle la méthode de cryptographie parfaite?

Transposition

Malheureusement, la réponse est négative.

Si l'algorithme de transposition aléatoire offre un niveau très élevé de sécurité, il pose aussi un vrai problème: …

Quelle est la clé de déchiffrement?

Le caractère aléatoire fait la force de la méthode, mais fait aussi sa faiblesse.

Substitution

Il faut donc trouver une autre méthode de chiffrement qui permet de générer des clés simples, faciles à retenir et à transmettre, sans trop sacrifier la sécurité.

↓

La substitution consiste à changer une lettre par une autre (ou par un symbole) indépendamment du fait que cette dernière se trouve dans le message ou non.

Polybe

Le chiffrement de Polybe est un des plus anciens chiffrements dont nous disposons d'informations détaillées sur son fonctionnement.

Il consiste à ranger les lettres de l'alphabet dans un tableau 5x5 et d'attribuer à chaque ligne et chaque colonne une lettre (par exemple A, B, C, D et E).

	A	**B**	**C**	**D**	**E**
A	A	B	C	D	E
B	F	G	H	I - J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Polybe

Chaque lettre d'un message est remplacée par la combinaison de lettre représentant sa ligne et sa colonne.

Le mot **ALARME** devient **AACAAADBCBAE**.

Le mot codé **CBAADDBCAECBAADDBDDADEAE** représente le mot …

	A	**B**	**C**	**D**	**E**
A	A	B	C	D	E
B	F	G	H	I - J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Polybe

Chaque lettre d'un message est remplacée par la combinaison de lettre représentant sa ligne et sa colonne.

Le mot **ALARME** devient **AACAAADBCBAE**.

Le mot codé **CBAADDBCAECBAADDBDDADEAE** représente le mot …

MATHEMATIQUE

	A	**B**	**C**	**D**	**E**
A	A	B	C	D	E
B	F	G	H	I - J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Chiffre de César

Le chiffre de César est un chiffrement par substitution qui consiste à assigner à une lettre de l'alphabet une autre lettre résultant du décalage de l'alphabet d'un certain nombre de lettres.

Il porte le nom de chiffre de César, parce qu'il était très utilisé par Jules César.

Chiffre de César

Par exemple, chaque lettre est remplacée par celle qui se trouve 3 positions plus loin dans l'alphabet.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Le mot **CESAR** devient **FHVDU**

Le message **QDPXU** représente …

Chiffre de César

Par exemple, chaque lettre est remplacée par celle qui se trouve 3 positions plus loin dans l'alphabet.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Le mot **CESAR** devient **FHVDU**

Le message **QDPXU** représente …

NAMUR

Chiffre de César

Lorsqu’un message est intercepté, le cryptanalyste, s’il connait l’algorithme, mais pas la clé doit tester toutes les combinaisons possibles.

Chiffre de César

Le message **RFSLJW** va être testé successivement par chaque alphabet jusqu'à ce qu'il représente un mot « possible »:

QERKIV

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

PDQJHU

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

OCPIGT

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

NBOHFS

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

MANGER

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Chiffre de César

Le problème principal du chiffre de César réside dans la pauvreté du nombre de clé.

A partir de l'alphabet français qui compte 26 lettres, nous ne disposons que de … 26 clés possibles.

Décrypter un message nécessite uniquement de tester les 26 alphabets

Arithmétique modulaire

Le chiffre de César peut être formalisé par un outil très commun des mathématiques: l'arithmétique modulaire.

L'arithmétique modulaire ou arithmétique de l'horloge constitue une base fondamentale des systèmes actuels de sécurité de l'information.

Arithmétique modulaire

Comparons une horloge analogique et une horloge numérique.

L'horloge analogique divise le cercle en douze parties.

L'équivalence entre une horloge analogique et une horloge numérique est donnée par le tableau suivant:

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23

Lorsqu'on dit qu'il est 16 heures, on dit également qu'il est 4 heures de l'après-midi.

Arithmétique modulaire

Ce principe est aussi utilisé pour les angles: un angle de 370° est équivalent à un angle de 10°

370° = 360° + 10° -> On retranche à 370°, un tour complet du cercle qui vaut 360°. Il reste donc 10°

On peut donc écrire que **370 = (1 x 360) + 10**

Ou que 10 est le **reste** de 370 **divisé** par 360

A combien de degré équivaut un angle de **750°**?

Arithmétique modulaire

Ce principe est aussi utilisé pour les angles: un angle de 370° est équivalent à un angle de 10°

370° = 360° + 10° -> On retranche à 370°, un tour complet du cercle qui vaut 360°. Il reste donc 10°

On peut donc écrire que **370 = (1 x 360) + 10**

Ou que 10 est le **reste** de 370 **divisé** par 360

A combien de degré équivaut un angle de **750°**?

30° -> 750 = 2 x 360 + 30 -> 30 est le reste de 750 divisé par 360

Arithmétique modulaire

750 = 2 x 360 + 30 -> 30 est le reste de 750 divisé par 360

Ce calcul peut se noter $\mathbf{750 \equiv 30\ (mod\ 360)}$

Qui se lit: 750 est congruent à 30 modulo 360.

Dans le cas de l'horloge, 14 heures -> $14 \equiv 2\ (mod\ 12)$

Arithmétique modulaire

$$a \equiv b \ (mod\ m)$$

Le reste de la division de a par m est b

où a, b, m sont des nombres entiers

Arithmétique modulaire

A quelle heure analogique correspondent 19 heures?

se traduit par

$$19 \equiv x \ (\ mod \ 12 \ )$$

Arithmétique modulaire

A quelle heure analogique correspondent 19 heures?

se traduit par

$$19 \equiv x \ (mod \ 12 \ )$$

$$\boldsymbol{x = 7}$$

Arithmétique modulaire

A quelle heure analogique correspondent 127 heures?

se traduit par

$$127 \equiv x \ (mod\ 12\ )$$

$$\boldsymbol{x = 7}$$

$$127 - 12 = 115$$
$$115 - 12 = 103$$
$$103 - 12 = 91$$
$$\ldots$$
$$19 - 12 = \mathbf{7}$$

Arithmétique modulaire

L'arithmétique modulaire permet aussi de traiter des nombres négatifs.

$$-44 \equiv x \ (mod\ 7)$$
$$x = 5$$

$$-44 + 7 = -37$$
$$-37 + 7 = -30$$
$$-30 + 7 = -23$$
$$-23 + 7 = -16$$
$$-16 + 7 = -9$$
$$-9 + 7 = -2$$
$$-2 + 7 = \mathbf{5}$$

Arithmétique modulaire

Quel est le lien entre l'arithmétique modulaire et le chiffrement de César?

Considérons, l'alphabet standard et l'alphabet décalé de 3 lettres:

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Arithmétique modulaire

La version chiffrée d'un caractère de rang **x** dans l'alphabet en clair est le caractère de rang **x+3** dans le même alphabet.

La fonction de chiffrement peut alors être définie comme

$$C(x) = (x + 3)(mod\ 26)$$

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Arithmétique modulaire

Le chiffrement du mot BLEU donne

B = 1 -> $C(1) = (1 + 3)(mod\ 26) = 4$ -> **E**

L = 11 -> $C(11) = (11 + 3)(mod\ 26) = 14$ -> **O**

E = 4 -> $C(4) = (4 + 3)(mod\ 26) = 7$ -> **H**

U = 20 -> $C(20) = (20 + 3)(mod\ 26) = 23$ -> **X**

Le message **BLEU** chiffré avec la clé **3** devient **EOHX**

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Arithmétique modulaire

De façon générale, si nous avons un alphabet à $\boldsymbol{n}$ caractères et que nous utilisons une clé de valeur $\boldsymbol{k}$, nous pouvons écrire

$$C(x) = (x + k)(mod\ n)$$

Arithmétique modulaire

Le déchiffrement du message consiste à exécuter l'opération inverse:

$$C^{-1}(x) = (x - k)(mod\ n)$$

Déchiffrer EOHX avec un chiffre de César de clé 3 et un alphabet de 26 caractères donne

E = 4 -> $C^{-1}(4) = (4 - 3)(mod\ 26) = 1$-> **B**

O = 14 -> $C^{-1}(14) = (14 - 3)(mod\ 26) = 11$-> **L**

H = 7 -> $C^{-1}(7) = (7 - 3)(mod\ 26) = 4$ -> **E**

X = 23 -> $C^{-1}(23) = (23 - 3)(mod\ 26) = 20$ -> **U**

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Arithmétique modulaire

On peut étendre la fonction de chiffrement à une fonction de la forme

$$C_{(a,b)}(x) = (a \cdot x + b)(mod\ n)$$

On parlera de chiffrement affine ($a \cdot x + b$ est une fonction affine)

a et b sont des nombres entiers inférieurs à n

La clé de chiffrement est déterminée par les deux nombres a et b

Dans le cas du chiffrement de César de l'exemple, $a = 1$ et $b = 3$

Arithmétique modulaire

Le chiffrement affine offre une meilleure sécurité que le chiffrement de César.

Le chiffrement de César offre 26 clés possibles. Le chiffrement affine offre $26 \cdot 26 = 676$ clés.

C’est mieux, mais pas encore suffisant pour ne pas empêcher les attaques par **force brute** (on essaye toutes les combinaisons).

Arithmétique modulaire

Existe-t-il des conditions pour rendre le déchiffrement possible? Aussi bien pour le destinataire, que pour un espion?

Imaginons un alphabet de six lettres.

0	1	2	3	4	5
A	B	C	D	E	F

Et chiffrons les messages avec la fonction $C(x) = (2x + 1)(mod\ 6)$

Arithmétique modulaire

0	1	2	3	4	5
A	B	C	D	E	F

La lettre A -> $C(0) = (2.0 + 1)(mod\ 6) = 1$ -> La lettre B

La lettre B -> $C(1) = (2.1 + 1)(mod\ 6) = 3$ -> La lettre D

La lettre C -> $C(2) = (2.2 + 1)(mod\ 6) = 5$ -> La lettre F

La lettre D -> $C(3) = (2.3 + 1)(mod\ 6) = 1$ -> La lettre B

La lettre E -> $C(4) = (2.4 + 1)(mod\ 6) = 3$ -> La lettre D

La lettre F -> $C(5) = (2.5 + 1)(mod\ 6) = 5$ -> La lettre F

« ABC » et « DEF » ont le même code !!!

Arithmétique modulaire

Il existe en réalité une condition pour rendre le déchiffrement possible.
Il faut que

$$pgcd(a, n) = 1$$

Or dans notre exemple, le $pgcd(2,6) = 2$

PGCD = Plus grand commun diviseur

Exemple

Voici un message crypté selon un chiffre affine $(7x + 1)$.

A B R B L A D , W B O X X V O D O X D H I A D
, D X E W F S F X D D D O E Q V F X C B Q E
F D X , W V O E A L O D D X E Y B I F E D D
C B Q A D X I D A R D X , A B L E Q D C B
Q A D X B J L F E B F O X , A B E Q V F X F D
H D C B Q P D L G J L F W B O X A D L Q
C Q V C Q D A B O R L D X D O V H H D O E P
D A E D X , D E , W B O X A B O V E Q D , R B L
A V F X

Exemple

Construisons notre tableau de déchiffrement:

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**

La fonction inverse s'écrit $C^{-1}(x) = \big(15(x-1)\big)(mod\ 26)$

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
11	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22
L	A	P	E	T	I	X	M	B	Q	F	U	J	Y	N	C	R	G	V	K	Z	O	D	S	H	W

Exemple

$$C(x) = (7x + 1)(mod\ 26)$$

$$\downarrow$$

$$C^{-1}(x) = (15(x - 1))(mod\ 26)$$

$$y = 7x + 1$$
$$7x = y - 1$$

Il faut trouver l'inverse de 7 modulo 26, c'est-à-dire un entier n tel que

$$n.7 \equiv 1(mod\ 26) \rightarrow 15$$
$$(15.7 = 105 \rightarrow 105(mod\ 26) = 1)$$

Exemple

A B R B L A D , W B O X X V O D O X D H I A D
, D X E W F S F X D D D O E Q V F X C B Q E
F D X , W V O E A L O D D X E Y B I F E D D
C B Q A D X I D A R D X , A B L E Q D C B
Q A D X B J L F E B F O X , A B E Q V F X F D
H D C B Q P D L G J L F W B O X A D L Q
C Q V C Q D A B O R L D X D O V H H D O E P
D A E D X , D E , W B O X A B O V E Q D , R B L
A V F X

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
11	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22
L	A	P	E	T	I	X	M	B	Q	F	U	J	Y	N	C	R	G	V	K	Z	O	D	S	H	W

Exemple

LA GAULE, DANS SON ENSEMBLE, EST DIVISEE EN TROIS PARTIES, DONT L'UNE EST HABITEE PAR LES BELGES, L'AUTRE PAR LES AQUITAINS, LA TROISIEME PAR CEUX QUI DANS LEUR PROPRE LANGUE SE NOMMENT CELTES, ET, DANS LA NOTRE, GAULOIS

« La Gaule, dans son ensemble, est divisée en trois parties, dont l'une est habitée par les Belges, l'autre par les Aquitains, la troisième par ceux qui dans leur propre langue se nomment Celtes, et, dans la nôtre, Gaulois » - La guerre des gaules – Jules César – Traduction Maurice Rat

Chiffre de César

Le chiffrement peut être considérablement sécurisé si on ne s'oblige plus à suivre l'ordre de l'alphabet.

Le nombre de clé passe ainsi de 26 à …

Chiffre de César

Le chiffrement peut être considérablement sécurisé si on ne s'oblige plus à suivre l'ordre de l'alphabet.

Le nombre de clé passe ainsi de 26 à …

26!=403.291.461.126.605.635.584.000.000 clés

Un espion qui essaierait une clé par seconde mettrait plus d'un milliard de fois la vie estimée de l'Univers avant d'épuiser toutes les possibilités.

Chiffre de César

Le nombre de clé est énorme, mais la transmission de la clé et sa mémorisation reste périlleux.

Pour rendre la transmission et la mémorisation plus simple, on pourrait par exemple utiliser l'ordonnancement des lettres selon un clavier AZERTY « belge »:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
A	Z	E	R	T	Y	U	I	O	P	Q	S	D	F	G	H	J	K	L	M	W	X	C	V	B	N

Chiffre de César

Une autre méthode consiste à prendre un mot clé tel que CODE JANVIER

On supprime les blancs et les lettres en double: CODEJANVIR

Ces lettres chiffrent les premières lettre de l'alphabet. Ensuite on continue dans l'ordre de l'alphabet en partant de la première lettre libre qui suit la dernière lettre du code:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
C	O	D	E	J	A	N	V	I	R	S	T	U	W	X	Y	Z	B	F	G	H	K	L	M	P	Q

Chiffre de César

Il est même possible de convenir avec le destinataire que le code évolue chaque mois

CODE JANVIER -> CODE FEVRIER -> CODE MARS -> CODE AVRIL -> …

Chiffre de César

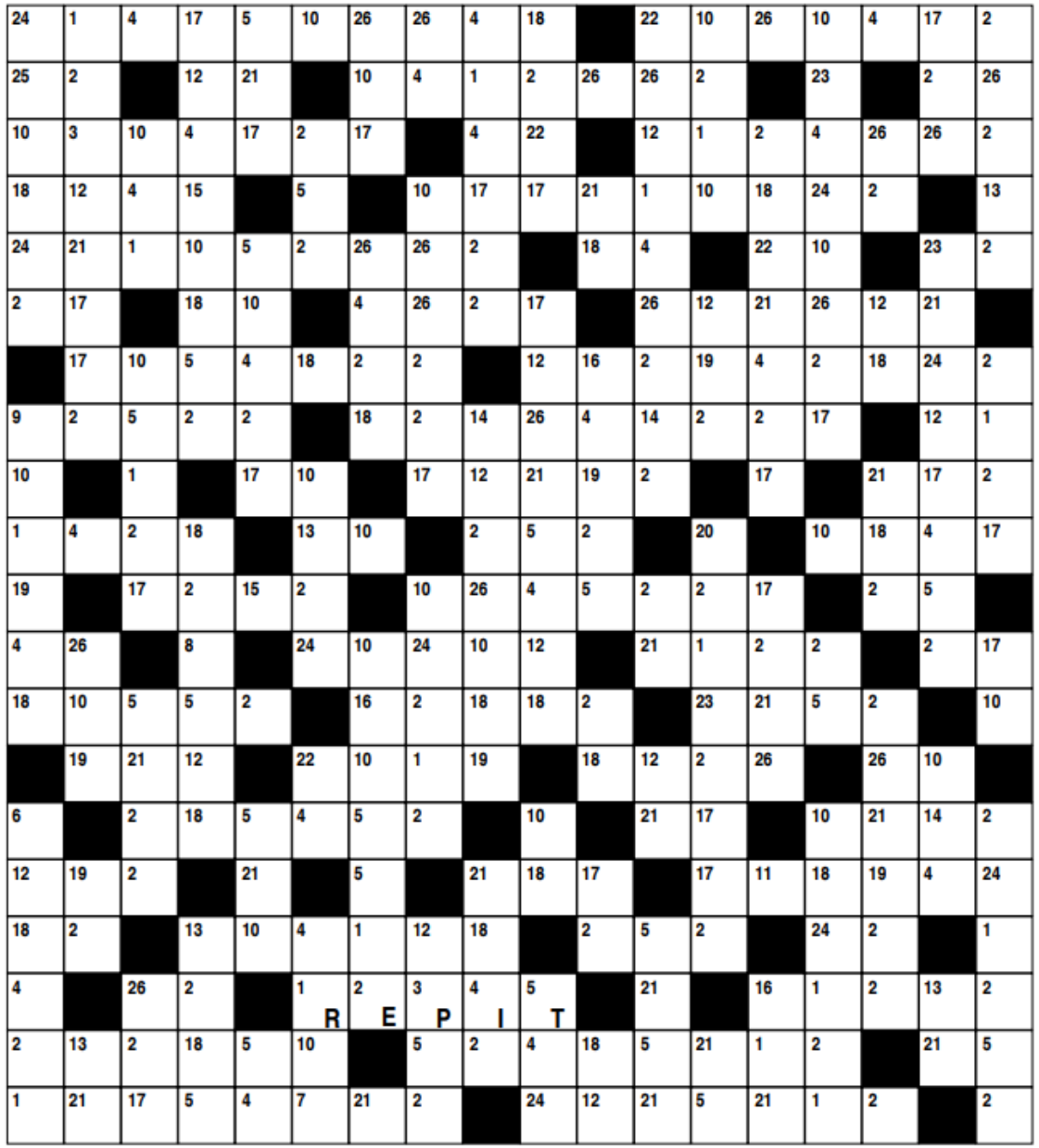
Cette méthode de chiffre est restée utilisée très longtemps.

La fiabilité du chiffre et la simplicité de l'algorithme ont longtemps donné un sentiment d'inviolabilité du chiffre.

Mais …

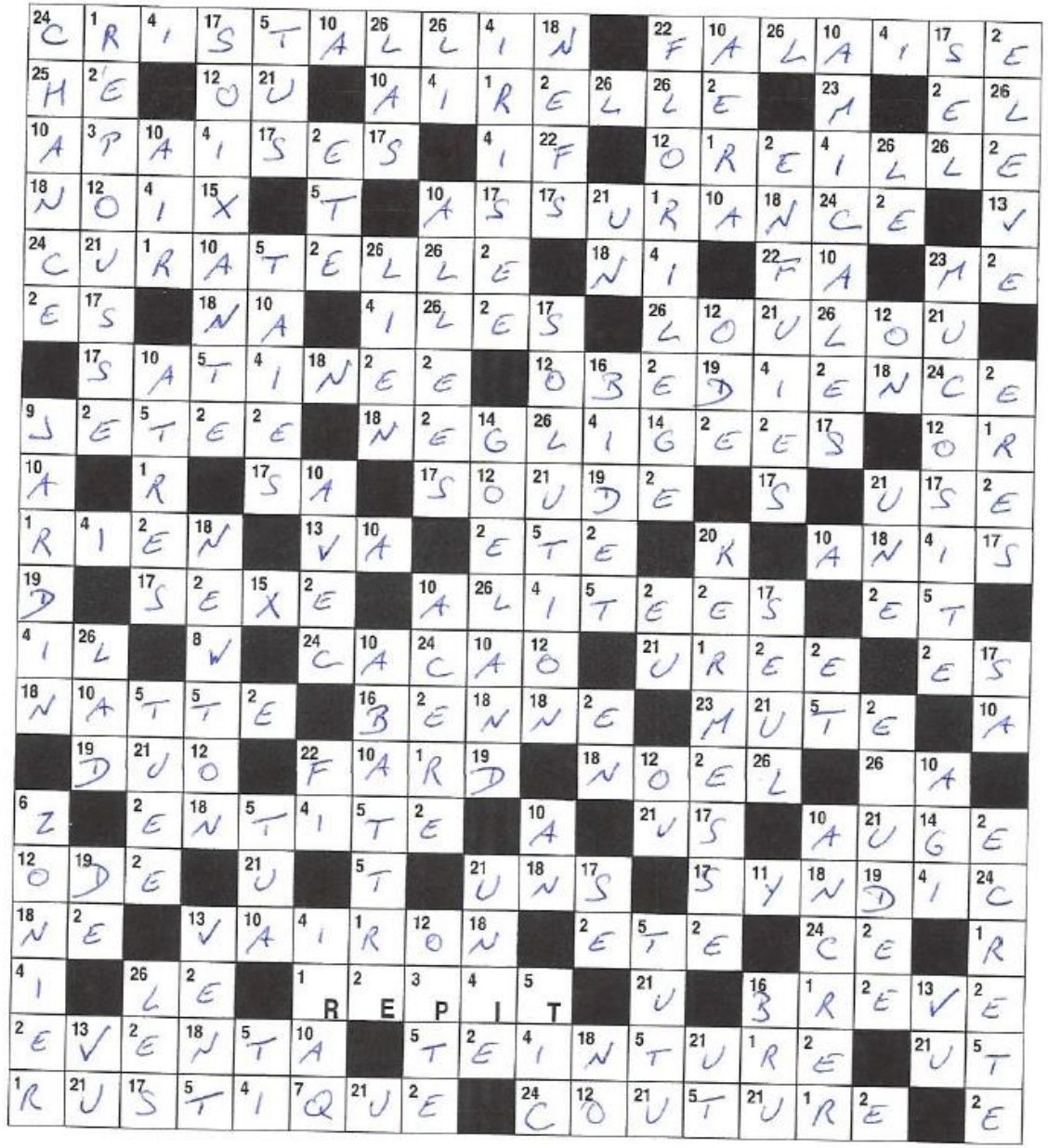
Mot codé

1	2	3	4	5	6	7	8	9	10	11	12	13
R	E	P	I	T								
14	15	16	17	18	19	20	21	22	23	24	25	26



Mot codé

1	2	3	4	5	6	7	8	9	10	11	12	13
R	E	P	I	T	Z	Q	W	J	A	Y	O	V
14	15	16	17	18	19	20	21	22	23	24	25	26
G	X	B	S	N	D	K	U	F	M	C	H	L



Substitution alphabétique

La substitution alphabétique repose sur le remplacement d'un caractère par un autre … toujours le même.

Hors dans une langue, chaque caractère est utilisé de façon inégale.

En français, si on analyse la fréquence d'apparition des lettres dans un texte suffisamment long, on va souvent trouvé que le E est la lettre la plus fréquente, suivie du S, A, I, …

Substitution alphabétique

Si on établit le tableau des fréquences on trouve par exemple:

A	9,42%	**N**	7,15%
B	1,02%	**O**	5,14%
C	2,64%	**P**	2,86%
D	3,39%	**Q**	1,06%
E	15,87%	**R**	6,46%
F	0,95%	**S**	7,90%
G	1,04%	**T**	7,26%
H	0,77%	**U**	6,24%
I	8,41%	**V**	2,15%
J	0,89%	**W**	≈ 0%
K	≈ 0%	**X**	0,30%
L	5,34%	**Y**	0,24%
M	3,24%	**Z**	0,32%

ESAINTRULODCPMVQGFHBXJYZKW

Substitution alphabétique

Donc lors de l'analyse d'un message crypté, on recense le nombre d'apparition de chaque caractère

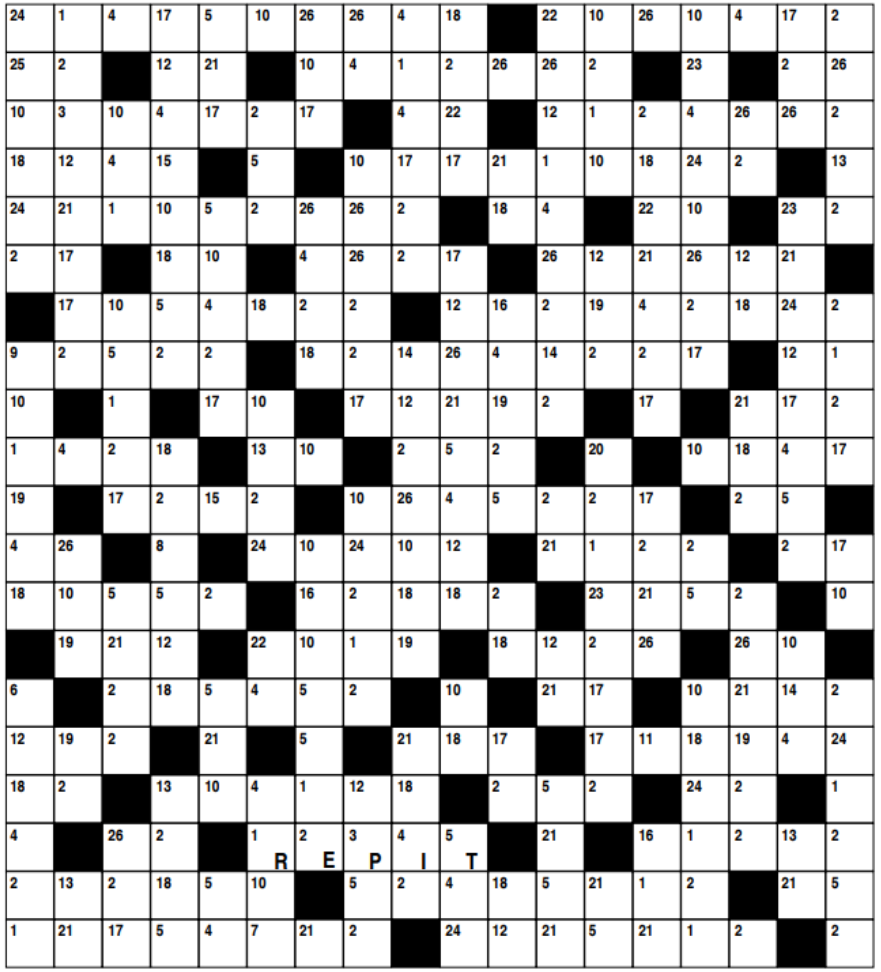
Le caractère qui est présent le plus souvent a beaucoup de chance d'être le « e »

Si cela ne marche pas, il pourrait s'agir du « a » ou du « i »

…

Substitution alphabétique

C’est le principe même de ce type de mot croisés



Substitution alphabétique

Examinons le message suivant

B Q P S N R S J X J N J X L D P C L D L P Q B E _ Q R
K J X H N K P K S J P J I K S P U N B D K I Q R B K P
Q P B Q P Z I T E J Q D Q B T S K P E L N I U N P H N
K P B K P C K S S Q W K P S L X J P S N V V X S Q C C
K D J P B L D W P X B P S N V V X J P G K P J K D X I
P Z L C E J K P G K S P S J Q J X S J X H N K S P G P
L Z Z N I K D Z K P G K S P G X V V K I K D J K S P B
K J J I K S

Substitution alphabétique

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

Message chiffré					
P	14,30%	D	4,60%	W	1,00%
K	12,80%	L	4,10%	U	1,00%
S	9,20%	V	3,10%	T	1,00%
J	9,20%	Z	2,60%	-	0,50%
X	5,60%	G	2,60%	O	0,00%
Q	5,60%	C	2,60%	M	0,00%
N	5,60%	E	2,00%	F	0,00%
B	5,10%	R	1,50%	A	0,00%
I	4,60%	H	1,50%	Y	0,00%

Substitution alphabétique

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

Message chiffré					
P	14,30%	D	4,60%	W	1,00%
K	12,80%	L	4,10%	U	1,00%
S	9,20%	V	3,10%	T	1,00%
J	9,20%	Z	2,60%	-	0,50%
X	5,60%	G	2,60%	O	0,00%
Q	5,60%	C	2,60%	M	0,00%
N	5,60%	E	2,00%	F	0,00%
B	5,10%	R	1,50%	A	0,00%
I	4,60%	H	1,50%	Y	0,00%

Remplaçons P par _

B Q _ S N R S J X J N J X L D _ C L D L _ Q B E _ Q R
K J X H N K _ K S J _ J I K S _ U N B D K I Q R B K _
Q _ B Q _ Z I T E J Q D Q B T S K _ E L N I U N _ H N
K _ B K _ C K S S Q W K _ S L X J _ S N V V X S Q C C
K D J _ B L D W _ X B _ S N V V X J _ G K _ J K D X I
_ Z L C E J K _ G K S _ S J Q J X S J X H N K S _ G _
L Z Z N I K D Z K _ G K S _ G X V V K I K D J K S _ B
K J J I K S

Substitution alphabétique

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

Message chiffré					
P	14,30%	D	4,60%	W	1,00%
K	12,80%	L	4,10%	U	1,00%
S	9,20%	V	3,10%	T	1,00%
J	9,20%	Z	2,60%	-	0,50%
X	5,60%	G	2,60%	O	0,00%
Q	5,60%	C	2,60%	M	0,00%
N	5,60%	E	2,00%	F	0,00%
B	5,10%	R	1,50%	A	0,00%
I	4,60%	H	1,50%	Y	0,00%

Remplaçons K par **E**

B Q _ S N R S J X J N J X L D _ C L D L _ Q B E _ Q R

E J X H N **E** _ **E** S J _ J I **E** S _ U N B D E I Q R B **E** _

Q _ B Q _ Z I T E J Q D Q B T S **E** _ E L N I U N _ H N

E _ B **E** _ C **E** S S Q W **E** _ S L X J _ S N V V X S Q C C

E D J _ B L D W _ X B _ S N V V X J _ G **E** _ J **E** D X I

_ Z L C E J **E** _ G **E** S _ S J Q J X S J X H N **E** S _ G _

L Z Z N I **E** D Z **E** _ G **E** S _ G X V V **E** I **E** D J **E** S _ B

E J J I **E** S

Substitution alphabétique

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

Message chiffré					
P	14,30%	D	4,60%	W	1,00%
K	12,80%	L	4,10%	U	1,00%
S	9,20%	V	3,10%	T	1,00%
J	9,20%	Z	2,60%	-	0,50%
X	5,60%	G	2,60%	O	0,00%
Q	5,60%	C	2,60%	M	0,00%
N	5,60%	E	2,00%	F	0,00%
B	5,10%	R	1,50%	A	0,00%
I	4,60%	H	1,50%	Y	0,00%

Remplaçons Q par **A**

B **A** _ S N R S J X J N J X L D _ C L D L _ **A** B E _ **A** R

E J X H N **E** _ **E** S J _ J I **E** S _ U N B D E I **A** R B **E** _

A _ B **A** _ Z I T E J **A** D **A** B T S **E** _ E L N I U N _ H N

E _ B **E** _ C **E** S S **A** W **E** _ S L X J _ S N V V X S **A** C C

E D J _ B L D W _ X B _ S N V V X J _ G **E** _ J **E** D X I

_ Z L C E J **E** _ G **E** S _ S J **A** J X S J X H N **E** S _ G _

L Z Z N I **E** D Z **E** _ G **E** S _ G X V V **E** I **E** D J **E** S _ B

E J J I **E** S

Substitution alphabétique

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

Message chiffré					
P	14,30%	D	4,60%	W	1,00%
K	12,80%	L	4,10%	U	1,00%
S	9,20%	V	3,10%	T	1,00%
J	9,20%	Z	2,60%	-	0,50%
X	5,60%	G	2,60%	O	0,00%
Q	5,60%	C	2,60%	M	0,00%
N	5,60%	E	2,00%	F	0,00%
B	5,10%	R	1,50%	A	0,00%
I	4,60%	H	1,50%	Y	0,00%

Remplaçons B par **L**

L **A** _ S N R S J X J N J X L D _ C L D L _ **A** **L** E _ **A** R

E J X H N **E** _ **E** S J _ J I **E** S _ U N **L** D E I **A** R **L** **E** _

A _ **L** **A** _ Z I T E J **A** D **A** **L** T S **E** _ E L N I U N _ H N

E _ **L** **E** _ C **E** S S **A** W **E** _ S L X J _ S N V V X S **A** C C

E D J _ **L** L D W _ X **L** _ S N V V X J _ G **E** _ J **E** D X I

_ Z L C E J **E** _ G **E** S _ S J **A** J X S J X H N **E** S _ G _

L Z Z N I **E** D Z **E** _ G **E** S _ G X V V **E** I **E** D J **E** S _ **L**

E J J I **E** S

Substitution alphabétique

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

Message chiffré					
P	14,30%	D	4,60%	W	1,00%
K	12,80%	L	4,10%	U	1,00%
S	9,20%	V	3,10%	T	1,00%
J	9,20%	Z	2,60%	-	0,50%
X	5,60%	G	2,60%	O	0,00%
Q	5,60%	C	2,60%	M	0,00%
N	5,60%	E	2,00%	F	0,00%
B	5,10%	R	1,50%	A	0,00%
I	4,60%	H	1,50%	Y	0,00%

Remplaçons S par **S**

L **A** **_** **S** N R **S** J X J N J X L D **_** C L D L **_** **A** **L** E **_** **A** R

E J X H N **E** **_** **E** **S** J **_** J I **E** **S** **_** U N **L** D E I **A** R **L** **E** **_**

A **_** **L** **A** **_** Z I T E J **A** D **A** **L** T **S** **E** **_** E L N I U N **_** H N

E **_** **L** **E** **_** C **E** **S** **S** **A** W **E** **_** **S** L X J **_** **S** N V V X **S** **A** C C

E D J **_** **L** L D W **_** X **L** **_** **S** N V V X J **_** G **E** **_** J **E** D X I

_ Z L C E J **E** **_** G **E** **S** **_** **S** J **A** J X **S** J X H N **E** **S** **_** G **_**

L Z Z N I **E** D Z **E** **_** G **E** **S** **_** G X V V **E** I **E** D J **E** **S** **_** **L**

E J J I **E** **S**

Substitution alphabétique

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

Message chiffré					
P	14,30%	D	4,60%	W	1,00%
K	12,80%	L	4,10%	U	1,00%
S	9,20%	V	3,10%	T	1,00%
J	9,20%	Z	2,60%	-	0,50%
X	5,60%	G	2,60%	O	0,00%
Q	5,60%	C	2,60%	M	0,00%
N	5,60%	E	2,00%	F	0,00%
B	5,10%	R	1,50%	A	0,00%
I	4,60%	H	1,50%	Y	0,00%

Remplaçons G par **D**

L A _ S N R **S** J X J N J X L D **_** C L D L **_** **A L** E **_** **A** R

E J X H N **E _ E S** J **_** J I **E S _** U N **L** D E I **A** R **L E _**

A _ L A _ Z I T E J **A** D **A L** T **S E _** E L N I U N **_** H N

E _ L E _ C **E S S A** W **E _ S** L X J **_** **S** N V V X **S A** C C

E D J **_ L** L D W **_** X **L _ S** N V V X J **_** **D E _** J **E** D X I

_ Z L C E J **E _ D E S _ S** J **A** J X **S** J X H N **E S _ D _**

L Z Z N I **E** D Z **E _ D E S _ D** X V V **E** I **E** D J **E S _ L**

E J J I **E S**

Substitution alphabétique

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

Message chiffré					
P	14,30%	D	4,60%	W	1,00%
K	12,80%	L	4,10%	U	1,00%
S	9,20%	V	3,10%	T	1,00%
J	9,20%	Z	2,60%	-	0,50%
X	5,60%	G	2,60%	O	0,00%
Q	5,60%	C	2,60%	M	0,00%
N	5,60%	E	2,00%	F	0,00%
B	5,10%	R	1,50%	A	0,00%
I	4,60%	H	1,50%	Y	0,00%

Remplaçons J par **T**

L A _ S N R **S T** X **T** N **T** X L D **_** C L D L **_ A L** E **_ A** R

E T X H N **E _ E S T _ T** I **E S _** U N **L** D E I **A** R **L E _**

A _ L A _ Z I T E **T A** D **A L** T **S E _** E L N I U N **_** H N

E _ L E _ C **E S S A** W **E _ S** L X **T _ S** N V V X **S A** C C

E D **T _ L** L D W **_** X **L _ S** N V V X **T _ D E _ T E** D X I

_ Z L C E **T E _ D E S _ S T A T** X **S T** X H N **E S _ D _**

L Z Z N I **E** D Z **E _ D E S _ D** X V V **E** I **E** D **T E S _ L**

E T T I **E S**

Substitution alphabétique

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

Message chiffré					
P	14,30%	D	4,60%	W	1,00%
K	12,80%	L	4,10%	U	1,00%
S	9,20%	V	3,10%	T	1,00%
J	9,20%	Z	2,60%	-	0,50%
X	5,60%	G	2,60%	O	0,00%
Q	5,60%	C	2,60%	M	0,00%
N	5,60%	E	2,00%	F	0,00%
B	5,10%	R	1,50%	A	0,00%
I	4,60%	H	1,50%	Y	0,00%

Remplaçons I par **R**

L A _ S N R **S T** X **T** N **T** X L D **_** C L D L **_ A L** E **_ A** R
E T X H N **E _ E S T _ T R E S _** U N **L** D E **R A** R **L E _**
A _ L A _ Z **R** T E **T A** D **A L** T **S E _** E L N **R** U N **_** H N
E _ L E _ C **E S S A** W **E _ S** L X **T _ S** N V V X **S A** C C
E D **T _ L** L D W **_** X **L _ S** N V V X **T _ D E _ T E** D X **R**
_ Z L C E **T E _ D E S _ S T A T** X **S T** X H N **E S _ D _**
L Z Z N **R E** D Z **E _ D E S _ D** X V V **E R E** D **T E S _ L**
E T T R E S

Substitution alphabétique

…

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

Message chiffré					
P	14,30%	D	4,60%	W	1,00%
K	12,80%	L	4,10%	U	1,00%
S	9,20%	V	3,10%	T	1,00%
J	9,20%	Z	2,60%	-	0,50%
X	5,60%	G	2,60%	O	0,00%
Q	5,60%	C	2,60%	M	0,00%
N	5,60%	E	2,00%	F	0,00%
B	5,10%	R	1,50%	A	0,00%
I	4,60%	H	1,50%	Y	0,00%

L A _ S U B S T I T U T I O N _ M O N O _ A L P H A B
E T I Q U E _ E S T _ T R E S _ V U L N E R A B L E _
A _ L A _ C R Y P T A N A L Y S E _ P O U R V U _ Q U
E _ L E _ M E S S A G E _ S O I T _ S U F F I S A M M
E N T _ L O N G _ I L _ S U F F I T _ D E _ T E N I R
_ C O M P T E _ D E S _ S T A T I S T I Q U E S _ D _
O C C U R E N C E _ D E S _ D I F F E R E N T E S _ L
E T T R E S

La substitution mono-alphabétique est très vulnérable à la cryptanalyse pourvu que le message soit suffisamment long. Il suffit de tenir compte des statistiques d'occurrence des différentes lettres.

Exercices

Français					
-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

H B F E Q D P V Q I D B L , X L Q L O
D C D Q P Y D , E D O B F E D O X V O
L O K Q V H B R D . H B F E Q D Q D O B
B Q A V W D L Q B A A D P Y D , A L F
E B C D L C Q D X P D A B O R B R
D I V O M V L Q , H V O X F D L Q W L
D B L . J L D S V L X D E D X M V A F
S V L X H D X D H I A D U I D B L !
H D O E F Q , X F S V E Q D Q B H B R D
Q B C C V Q E D B S V E Q D C A L H B

Exercice

A	8	J	1	S	4
B	18	K	1	T	0
C	6	L	16	U	1
D	31	M	2	V	13
E	10	N	0	W	2
F	8	O	10	X	9
G	0	P	4	Y	2
H	9	Q	18	Z	0
I	4	R	4		

Français

-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

H B F E Q D P V Q I D B L , X L Q L O
D C D Q P Y D , E D O B F E D O X V O
L O K Q V H B R D . H B F E Q D Q D O B
B Q A V W D L Q B A A D P Y D , A L F
E B C D L C Q D X P D A B O R B R
D I V O M V L Q , H V O X F D L Q W L
D B L . J L D S V L X D E D X M V A F
S V L X H D X D H I A D U I D B L !
H D O E F Q , X F S V E Q D Q B H B R D
Q B C C V Q E D B S V E Q D C A L H B

Exercice

M A I T R E C O R B E A U , S U R U N
E P E R C H E , T E N A I T E N S O N
U N F R O M A G E . M A I T R E R E N A
A R L ' O D E U R A L L E C H E , L U I
T A P E U P R E S C E L A N G A G
E B O N J O U R , M O N S I E U R D U
E A U . Q U E V O U S E T E S J O L I
V O U S M E S E M B L E Z B E A U !
M E N T I R , S I V O T R E R A M A G E
R A P P O R T E A V O T R E P L U M A

Maître Corbeau, sur un arbre perché, tenait en son bec un fromage. Maître Renard, par l'odeur alléché, lui tint à peu près ce langage: « Hé! Bonjour, Monsieur du Corbeau. Que vous êtes joli! Que vous me semblez beau! Sans mentir, si votre ramage se rapporte à votre plumage, vous êtes la Phénix des hôtes de ces bois. » … Le Corbeau et le Renard – Jean de La Fontaine

Exercice

A	15	J	0	S	6
B	29	K	26	T	0
C	2	L	18	U	0
D	22	M	0	V	0
E	3	N	2	W	8
F	0	O	21	X	0
G	0	P	10	Y	4
H	0	Q	1	Z	6
I	0	R	24		

Français

-	19,30%	L	4,70%	H	0,80%
E	10,90%	O	4,10%	G	0,80%
A	6,70%	D	2,90%	B	0,60%
S	6,30%	P	2,50%	X	0,40%
I	6,10%	C	2,40%	Y	0,30%
T	6,10%	M	2,10%	J	0,30%
N	5,60%	V	1,30%	Z	0,10%
R	5,30%	Q	1,30%	K	0%
U	5,20%	F	0,90%	W	0%

P O E D R L R O K D Z S B A R L L B O A K B
K K D Z S B N O B B K B K D O L P K A B A R D
O B K C D S R A B K K D K C R O . R K L D
O O B L D O O D Z , L D O W B O N L R Z Z
B A W R K P K B A R D O B K B L L D K R B A R
D O L P A W B E B R K . D O K R O E R A B
B L P Q R W B P L K P K A B A R D O , S B K S B
A R D O , S P R L W B L R D . R K Y P A L ' B
K K D W L . D O K ' R O Y D W Z B : L D P Y Y W B
R A - R K ?

Exercice

UN VOISIN COMPATISSANT L'ACCOMPAGNA A LA CONSULTATION A L'HOPITAL COCHIN. IL DONNA SON NOM, SON RANG D'IMMATRICULATION A L'ASSOCIATION DE TRAVAIL. ON L'INVITA A SUBIR AUSCULTATION, PALPATION, PUIS RADIO. IL FUT D'ACCORD. ON L'INFORMA: SOUFFRAIT-IL?

« Un voisin compatissant l'accompagna à la consultation à l'hôpital Cochin. Il donna son nom, son rang d'immatriculation à l'association de travail. On l'invita à subir auscultation, palpation, puis radio. Il fut d'accord. On l'informa: souffrait-il? » La disparition – Georges Perec